sub a7

What is claimed is:

1. A computer program product for enabling an identity change during a certificate-based host access session, said computer program product embodied on a computer-readable medium and comprising:

computer-readable program code means for processing a first sign-on during a secure session using a digital certificate, further comprising:

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol;

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

computer-readable program code means for using said passed or retrieved digital certificate to locate access credentials for said user;

computer-readable program code means for accessing a stored password or generating a password substitute representing said located credentials; and

computer-readable program code means for using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

computer-readable program code means for processing a second sign-on during said secure session using a second digital certificate for a second identity, wherein said second sign-on requests access to said secure legacy host application or a different legacy host application by said user or by a different user, further comprising:

computer-readable program code means for receiving a second sign-on request using said second digital certificate for said second identity;

computer-readable program code means for passing said second digital certificate or a second certificate reference from said server machine to said host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

computer-readable program code means, operable in said host access security system, for using said passed second digital certificate or said second retrieved certificate to locate second access credentials;

computer-readable program code means for accessing a second stored password or generating a second password substitute representing said second credentials; and

computer-readable program code means for using said second stored password or said second password substitute to transparently complete said second sign-on to said secure legacy host application executing at said host system or said different legacy host application.

2. The computer program product as claimed in Claim 1, wherein said digital certificate is an X.509 certificate and said digital certificate reference and second certificate reference are references to an X.509 certificate.

3. The computer program product as claimed in Claim 1, wherein said communication protocol is a 3270 emulation protocol.

4. The computer program product as claimed in Claim 1, wherein said communication protocol is a 5250 emulation protocol.

5. The computer program product as claimed in Claim 1, wherein said communication protocol is a Virtual Terminal protocol.

6. The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

7. The computer program product as claimed in Claim 1, wherein said computer-readable program code means for processing said second sign-on further comprises computer-readable program code means for storing said second digital certificate.

8. The computer program product as claimed in Claim 1, wherein:

said computer-readable program code means for processing said first sign-on further comprises:

computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user;

computer-readable program code means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

computer-readable program code means for substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders in said first sign-on message; and

said computer-readable program code means for processing said second sign-on further comprises:

computer-readable program code means for requesting, by said legacy host application, second sign-on information for said second identity;

computer-readable program code means for responding to said request for second sign-on information by sending a second sign-on message with placeholders from said client machine to said server machine, said placeholders representing a different user identification and a different password of said second identity; and

computer-readable program code means for substituting said second user identifier associated with said second access credentials and said second stored password or said

second password substitute for said placeholders in said second sign-on message.

9. A system for enabling an identity change during a certificate-based host access session, comprising:

means for processing a first sign-on during a secure session using a digital certificate, further comprising:

means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

means for storing said digital certificate or a reference thereto at said server machine;

means for establishing a session from said server machine to a host system using a legacy host communication protocol;

means for passing said stored digital certificate or said reference from said server machine to a host access security system;

means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

means for using said passed or retrieved digital certificate to locate access credentials for said user;

means for accessing a stored password or generating a password substitute representing said located credentials; and

means for using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

means for processing a second sign-on during said secure session using a second digital certificate for a second identity, wherein said second sign-on requests access to said secure legacy host application or a different legacy host application by said user or by a different user, further comprising:

means for receiving a second sign-on request using said second digital certificate for said second identity;

means for passing said second digital certificate or a second certificate reference from said server machine to said host access security system;

means, operable in said host access security system, for authenticating said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

means, operable in said host access security system, for using said passed second digital certificate or said second retrieved certificate to locate second access credentials;

means for accessing a second stored password or generating a second password substitute representing said second credentials; and

means for using said second stored password or said second password substitute to transparently complete said second sign-on to said secure legacy host application executing at said host system or said different legacy host application.

10. The system as claimed in Claim 9, wherein said digital certificate is an X.509 certificate and said digital certificate reference and second certificate reference are references to an X.509 certificate.

11. The system as claimed in Claim 9, wherein said communication protocol is a 3270 emulation protocol.

12. The system as claimed in Claim 11, wherein said host access security system is a Resource Access Control Facility (RACF) system.

13. The system as claimed in Claim 9, wherein said means for processing said second sign-on further comprises means for storing said second digital certificate.

14. The system as claimed in Claim 9, wherein:

said means for processing said first sign-on further comprises:

means for requesting by said legacy host application, responsive to said means for establishing said session, first sign-on information for said user;

means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

means for substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders

in said first sign-on message; and

said means for processing said second sign-on further comprises:

means for requesting, by said legacy host application, second sign-on information for said second identity;

means for responding to said request for second sign-on information by sending a second sign-on message with placeholders from said client machine to said server machine, said placeholders representing a different user identification and a different password of said second identity; and

means for substituting said second user identifier associated with said second access credentials and said second stored password or said second password substitute for said placeholders in said second sign-on message.

15. A method for enabling an identity change during a certificate-based host access session, comprising the steps of:

processing a first sign-on during a secure session using a digital certificate, further comprising the steps of:

establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

storing said digital certificate or a reference thereto at said server machine;

establishing a session from said server machine to a host system using a legacy host communication protocol;

passing said stored digital certificate or said reference from said server machine to a host access security system;

authenticating, by said host access security system, said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

using said passed or retrieved digital certificate to locate access credentials for said user;

accessing a stored password or generating a password substitute representing said located credentials; and

using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

processing a second sign-on during said secure session using a second digital certificate for a second identity, wherein said second sign-on requests access to said secure legacy host application or a different legacy host application by said user or by a different user, further comprising the steps of:

receiving a second sign-on request using said second digital certificate for said second identity;

passing said second digital certificate or a second certificate reference from said server machine to said host access security system;

authenticating, by said host access security system, said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

using, by said host access security system, said passed second digital certificate or

said second retrieved certificate to locate second access credentials;

accessing a second stored password or generating a second password substitute representing said second credentials; and

using said second stored password or said second password substitute to transparently complete said second sign-on to said secure legacy host application executing at said host system or said different legacy host application.

16. The method as claimed in Claim 15, wherein said digital certificate is an X.509 certificate and said digital certificate reference and second certificate reference are references to an X.509 certificate.

17. The method as claimed in Claim 15, wherein said communication protocol is a 3270 emulation protocol.

18. The method as claimed in Claim 17, wherein said host access security system is a Resource Access Control Facility (RACF) system.

19. The method as claimed in Claim 15, wherein said step of processing said second sign-on further comprises the step of storing said second digital certificate.

20. The method as claimed in Claim 15, wherein:

said step of processing said first sign-on further comprises the steps of:

requesting by said legacy host application, responsive to said step of establishing said session, first sign-on information for said user;

responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders in said first sign-on message; and

said step of processing said second sign-on further comprises the steps of:

requesting, by said legacy host application, second sign-on information for said second identity;

responding to said request for second sign-on information by sending a second sign-on message with placeholders from said client machine to said server machine, said placeholders representing a different user identification and a different password of said second identity; and

substituting said second user identifier associated with said second access credentials and said second stored password or said second password substitute for said placeholders in said second sign-on message.